

IN THE CLAIMS:

Amended claims follow:

1. (Cancelled)
2. (Currently Amended) The method of claim 13, wherein one of said plurality of authentication tags is generated using a hash-based message authentication code algorithm.
3. (Currently Amended) ~~The method of claim 1,~~ An authentication method, comprising:
(a) generating a plurality of authentication tags for a message, each of said plurality of authentication tags reflecting a different authentication strength; and
(b) transmitting said plurality of authentication tags in association with said message to at least one receiver;
wherein one of said plurality of authentication tags is generated using a universal message authentication code algorithm.
4. (Currently Amended) The method of claim 13, wherein one of said plurality of authentication tags is generated using a partial message authentication code algorithm.
5. (Currently Amended) ~~The method of claim 1,~~ An authentication method, comprising:
(a) generating a plurality of authentication tags for a message, each of said plurality of authentication tags reflecting a different authentication strength; and

Docket: NAI1P080_99.123.01

-2-

(b) transmitting said plurality of authentication tags in association with said message to at least one receiver;

_____ wherein two or more of said plurality of authentication tags are generated using a nested structure that includes a plurality of inner functions that are each operative on a particular collection of message parts to produce a plurality of intermediate hash results, wherein a plurality of distinct combinations of one or more of said plurality of intermediate hash results are used by an outer hash function to produce said two or more authentication tags.

6. (Currently Amended) The method of claim ~~13~~, wherein said plurality of authentication tags are appended to said message.

7. (Original) An authentication method, comprising:

- (a) generating a plurality of collections of parts of said message;
- (b) processing each of said plurality of collections of message parts using a respective inner hash function to produce a plurality of intermediate hash results;
- (c) processing a plurality of distinct combinations of said plurality of intermediate hash results using an outer hash function to produce a plurality of authentication tags; and
- (d) transmitting said plurality of authentication tags in association with said message to at least one receiver.

8. (Original) The method of claim 7, wherein said plurality of collections of parts of said message are distinct.

9. (Original) The method of claim 7, wherein a collection of parts of said message is a collection of bits.

10. (Original) The method of claim 7, wherein a single inner hash function is used to create said plurality of intermediate hash results.

11. (Original) The method of claim 7, wherein two inner functions are used to produce a first and a second intermediate hash result, wherein said first intermediate hash result is processed using an outer function to produce a first authentication tag, said second intermediate hash result is processed using said outer function to produce a second authentication tag, and said first and second intermediate hash results are processed using said outer function to produce a third authentication tag.

12. – 15 (Cancelled)

16. (New) The method of claim 3, wherein the method is carried out utilizing a system including a manager.

17. (New) The method of claim 3, wherein the method is carried out utilizing a system including a local security and resource manager.

18. (New) The method of claim 3, wherein the method is carried out utilizing a system including a network application.

19. (New) The method of claim 3, wherein the method is carried out utilizing a system including a security association and key management module.

20. (New) The method of claim 3, wherein the method is carried out utilizing a system including a security services module.

21. (New) The system of claim 20, wherein the security services module includes a partial authentication portion.

22. (New) The system of claim 20, wherein the security services module includes a higher-speed lower-strength portion.

23. (New) The system of claim 20, wherein the security services module includes a lower-speed higher-strength portion.

24. (New) The method of claim 7, wherein the method is carried out utilizing a system including a local security and resource manager.

25. (New) The method of claim 7, wherein the method is carried out utilizing a system including a network application.

26. (New) The method of claim 7, wherein the method is carried out utilizing a system including a security association and key management module.

27. (New) The method of claim 7, wherein the method is carried out utilizing a system including a security services module.

28. (New) The method of claim 27, wherein the security services module includes a partial authentication portion.

29. (New) The method of claim 28, wherein the security services module includes a higher-speed lower-strength portion.

30. (New) The method of claim 29, wherein the security services module includes a lower-speed higher-strength portion.